Public Key Infrastructure

Roadmap
&
Certificate Policy

Mr. Gary Dahlquist
NSA / V51
(410) 854-4537
gndahlq@missi.ncsc.mil

13 May 1999

TOPICS

- Background
  - Information Assurance Services supported by Public Key Technology
  - PKI Assurance levels / Usage
- US DOD Certificate Policy
  - DoD Assurance Levels
  - Proposed DoD Usage
- DOD PKI Activities
  - Overview / User Registration
  - Status / Concerns
- Target DOD PKI (Roadmap)
  - Goals/Objectives
  - Overview of Target
  - Schedule
- Summary

Information Assurance Services & Public Key Technology

PKI supports Public key based technologies

Digital Signature	⟷	I&A, Integrity & Non-Repudiation
Key Encryption / Agreement	⟷	Confidentiality and Privacy

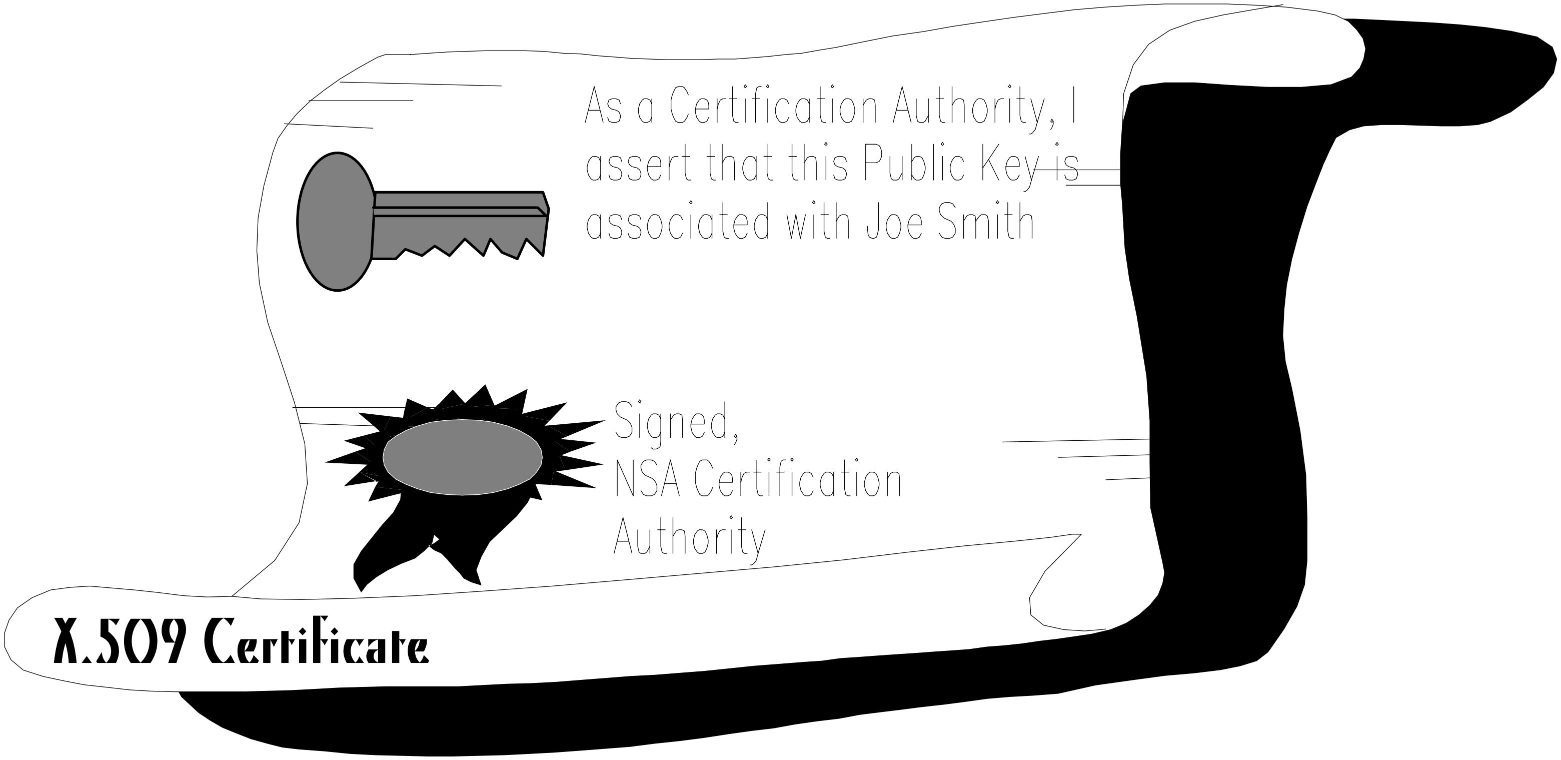
Information assurance services supported

Identification & Authentication (I&A) Authorization Access Control	⟷	Signature Verification Of Originator What Can They Do With What System Resources
Integrity	⟷	Protects Against Data Modification
Non-Repudiation	⟷	Proof Of Participation
Confidentiality	⟷	Privacy Of Data

A Public Key Certificate

Cryptographically binds an identity to a public key

Level of assurance of a certificate is the degree of confidence in this binding


As a Certification Authority, I assert that this Public Key is associated with Joe Smith
Signed,
NSA Certification Authority
X.509 Certificate

PKI Assurance Levels

- Strength of the cryptography
  - Algorithm and key sizes
- Form & protection of private key material
  - Type of token (e.g. Hardware, software)
  - Evaluated Assurance level (e.g. FIPS 140-1)
- Processes & controls employed in the operation of the PKI
  - Personnel, physical, procedural and technical security control employed by the PKI including registration

Assurance Level Usage

Based on:

- Value of the information;
- Level of risk;
- Consequences of loss, disclosure or modification;
- Reliance on PKI/certificates to provide the security services required.

DoD Assurance Levels

(Defined in the DoD X.509 Certificate Policy)

End User Perspective:

Class	User Identification	User Token	Algorithms
2 (Basic)	Not in person	Software	Type II
3 (Medium)	In person	Software	Type II
4 (High)	In person	Hardware (SmartCards/FORTEZZA)	Type II
5 (Classified)	In person	Hardware (STE FORTEZZA Plus card)	Type I

PKI:

- ***Personnel, physical, procedures, and technical security controls also play into assurance level (e.g. Revocation period, Re-key/renewal periods, auditing requirements, etc.)***

- ***Assurance of PKI must be greater than or equal to the assurance level of the certificates it issues (e.g. Class 3 PKI can issue Class 2 and 3 user certificates)***

Proposed DoD Certificate Usage

DIGITAL SIGNATURE

Criticality of Information

	Mission Support / Administrative	Mission Critical / National Security
Encrypted Network	**Class 3**	**Class 3**
Unencrypted Network	**Class 3**	**Class 4**

KEY EXCHANGE

Sensitivity of Information

	Classified Information	Mission Support / Administrative	Mission Critical / National Security / Communities of Interest
Encrypted Network	Class 3	Class 3	Class 3 / 4
Unencrypted Network	Class 5	Class 3	Class 4

DOD PKI Activities

- History
- Current Activities Overview
- Current Implementations
  - Overview / Status
    - High Assurance
    - Medium Assurance Pilot
- Concerns

History

Jan 93	MISSI / FORTEZZA PKI Development started
Mar 95	MISSI / FORTEZZA PKI Operational
Fall 96	Defense Travel System (DTS) needs digital signature
May 97	Multiple assurance level concept proposed
	High: MISSI / FORTEZZA
	Medium: Evaluated Commercial products/standards
Aug 97	MRM #16 directs DISA and NSA to implement DOD PKI
Aug 97	Joint Key Management Infrastructure Working Group expanded to formally include PKI
Oct 97	DISA/NSA host PKI Symposium

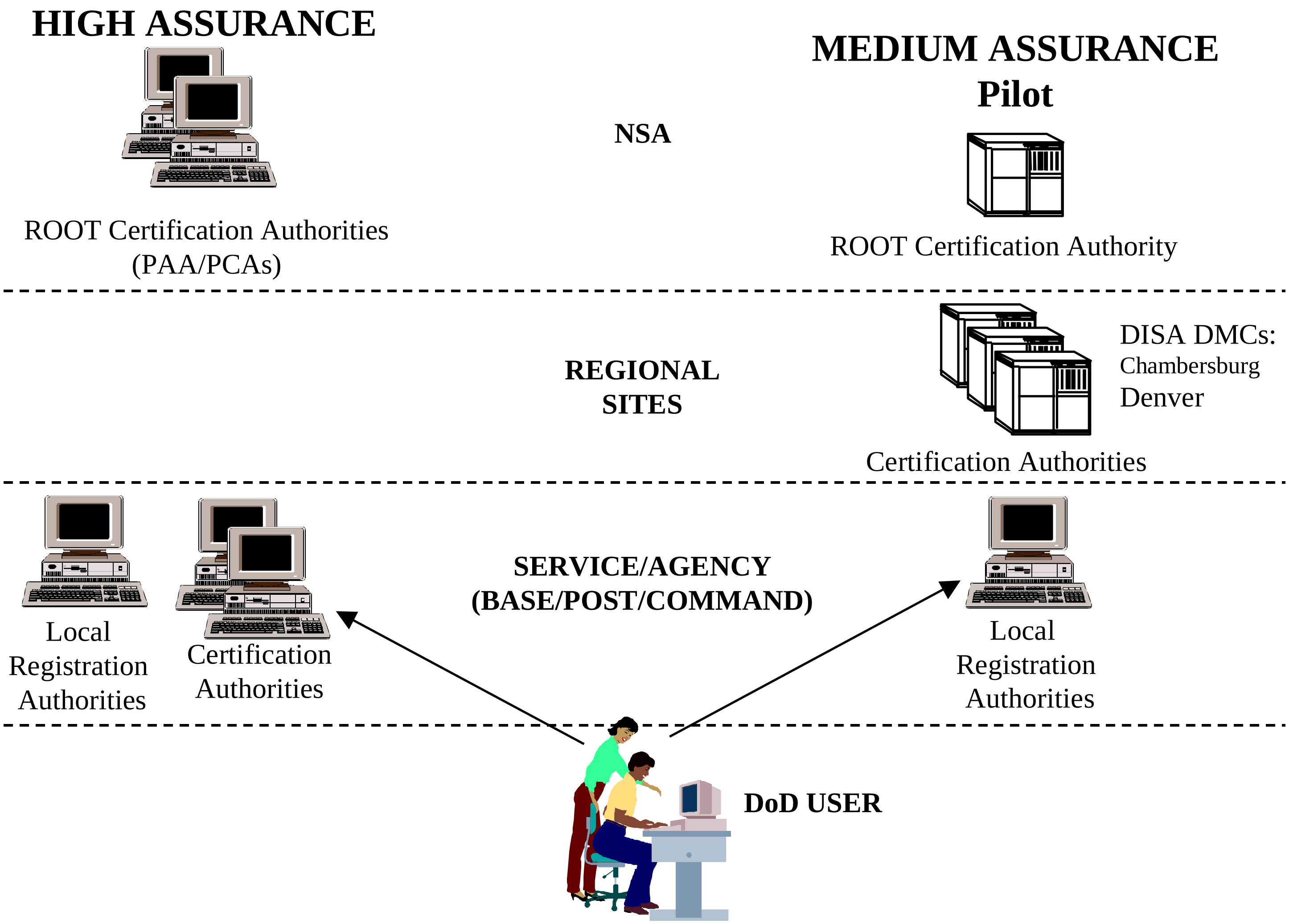
History (continued)

Jan 98	DOD Service/Agency PKI WG chartered to work medium assurance PKI
Jan 98	MISSI / FORTEZZA CAWs begin fielding to support DMS operationally
Feb 98	DISA conducts Defense-wide PKI survey
Apr 98	Pilot DOD Medium Assurance PKI operational
Sep 98	DOD Certificate Policy and Road Map sent to Services for review and comment
Nov 98	Comments from review sent to NSA / DISA

Current Activities Overview

- MISSI/FORTEZZA PKI
  - NSA / DISA developed Certificate Management and Directory Services components
  - Designed to support Defense Message System and other applications requiring ID and privilege information (I.e. attributes such as clearance, signature authority, nationality, special accesses)
- Medium Assurance Pilot PKI
  - Based on COTS technology
  - Designed to support the DOD Travel System (DTS) and other applications requiring identity certificates only

Current Implementations



HIGH ASSURANCE

ROOT Certification Authorities
(PAA/PCAs)

NSA

MEDIUM ASSURANCE
Pilot

ROOT Certification Authority

REGIONAL SITES

DISA DMCs:
Chambersburg
Denver

Certification Authorities

Local Registration Authorities

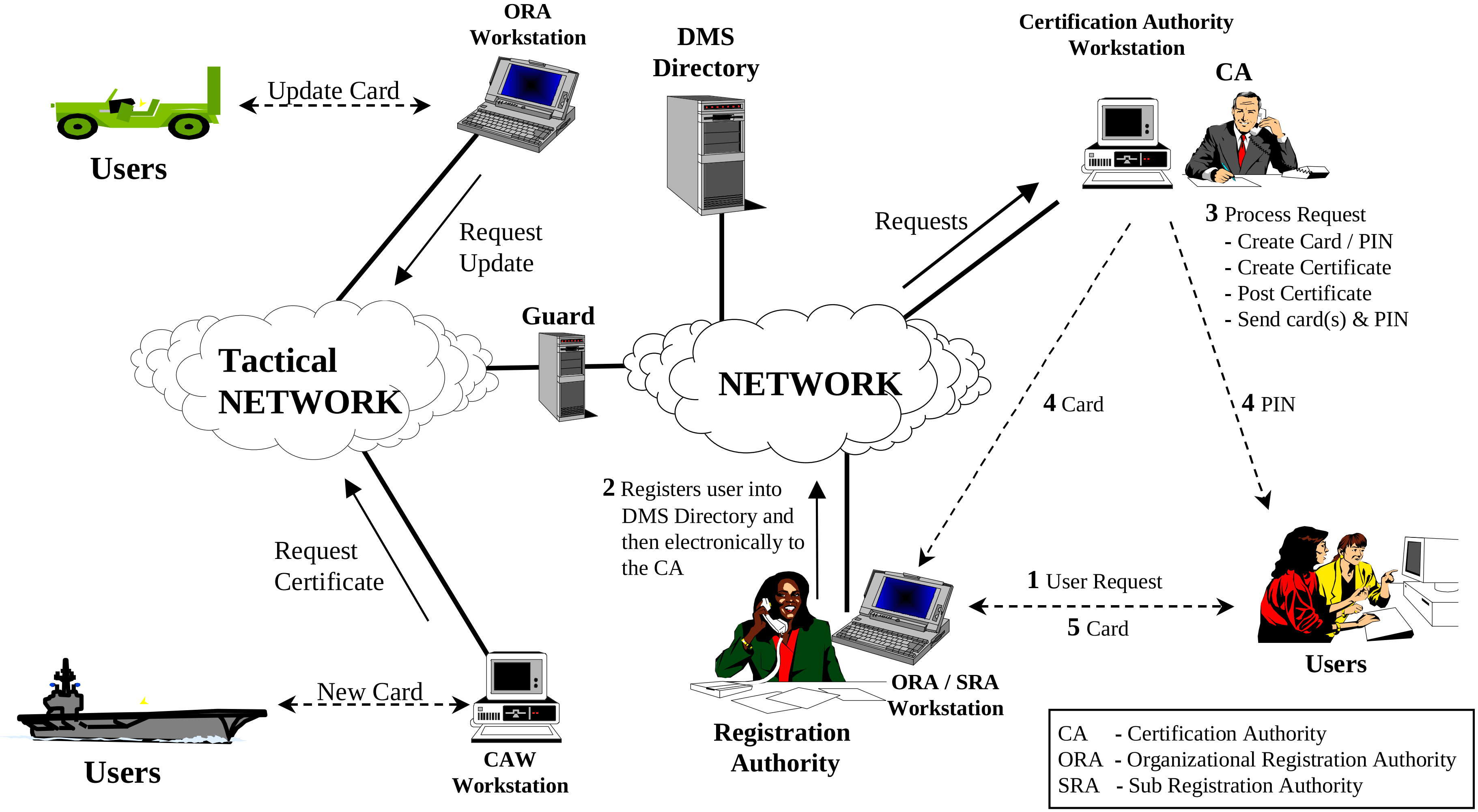
Certification Authorities

SERVICE/AGENCY (BASE/POST/COMMAND)

Local Registration Authorities

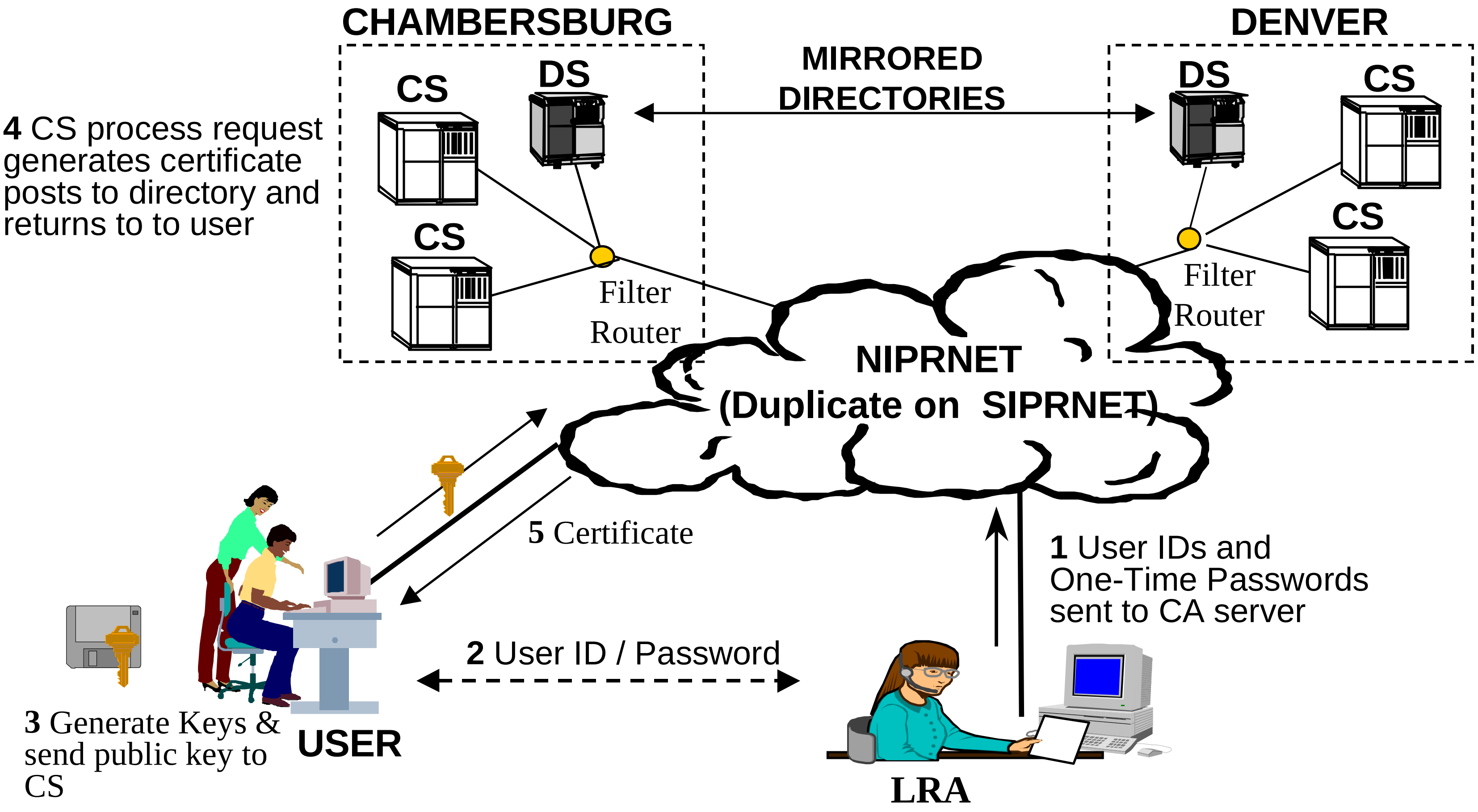
DoD USER

High Assurance PKI User Registration



CA - Certification Authority
ORA - Organizational Registration Authority
SRA - Sub Registration Authority

Medium Assurance PKI Pilot User Registration



CHAMBERSBURG

DENVER

MIRRORED DIRECTORIES

4 CS process request generates certificate posts to directory and returns to user

5 Certificate

1 User IDs and One-Time Passwords sent to CA server

2 User ID / Password

3 Generate Keys & send public key to CS

6 Export to Floppy

LEGEND

CS	-	Certificate Server
DS	-	Directory Server
LRA	-	Local Registration Authority

Medium Assurance PKI Pilot Security Status

- NSA has completed a system security assessment
  - Focused on PKI Components and user registration process
    - Certificate Server / Registration Authority (RA) / Local Registration Authority (LRA)
    - Directory Server
    - End user Browser for registration
  - Technical, physical, procedural and personnel recommendations being implemented
- NSA will reassess and certify each major release

Service / Agency PKI Concerns

- Near Term
  - – Resources to operate High Assurance Certification Authority Workstations
  - – Resources to operate Local Registration Authorities and the required in person registration
- Long Term
  - – Resources to operate multiple separate infrastructures

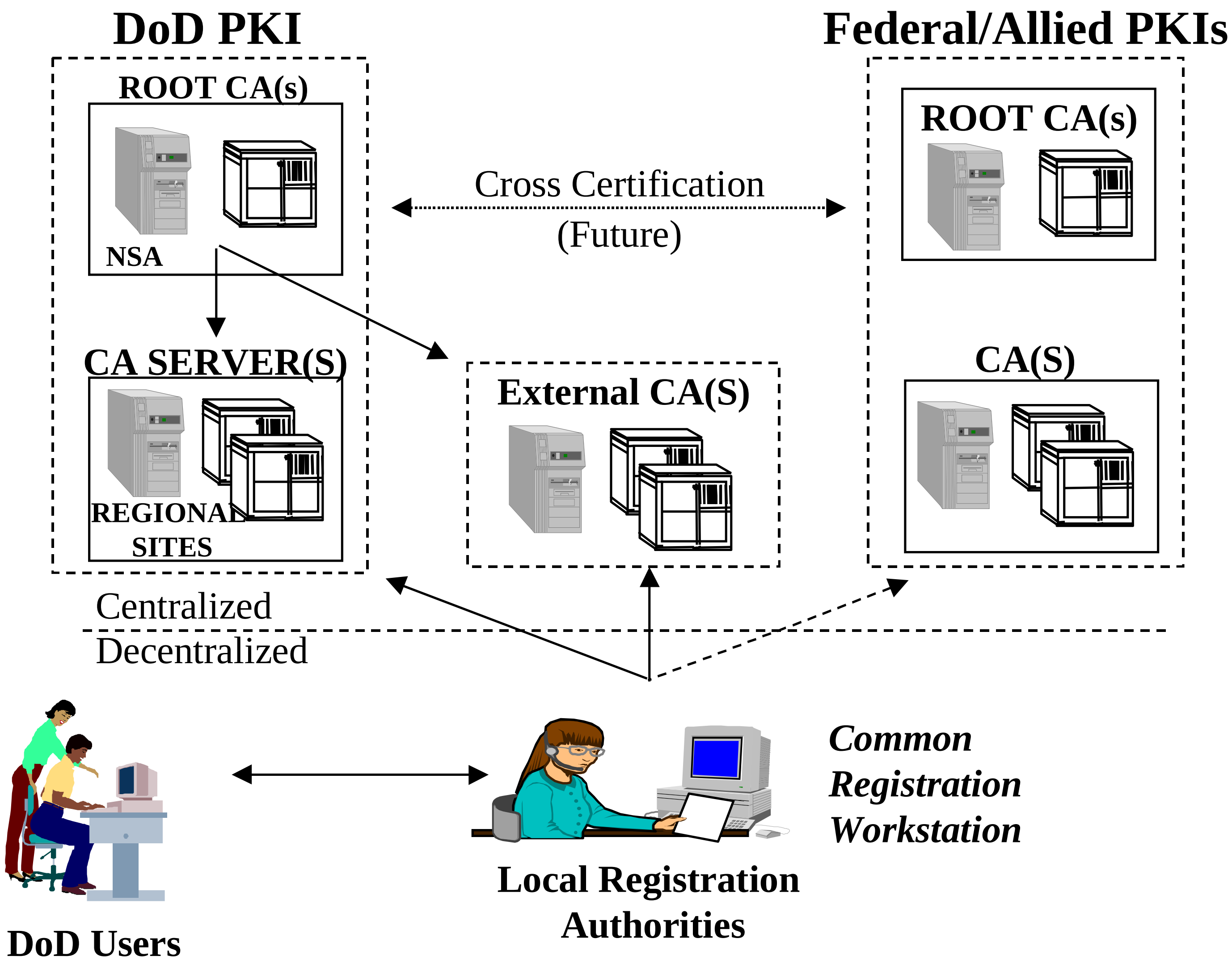
DOD Target PKI
(Roadmap)

- Goals / Objectives
- Architecture
- User Registration
- Technical Complexities
- Strategy for establishing Target DOD PKI
- Schedule (PKI & User Registration)

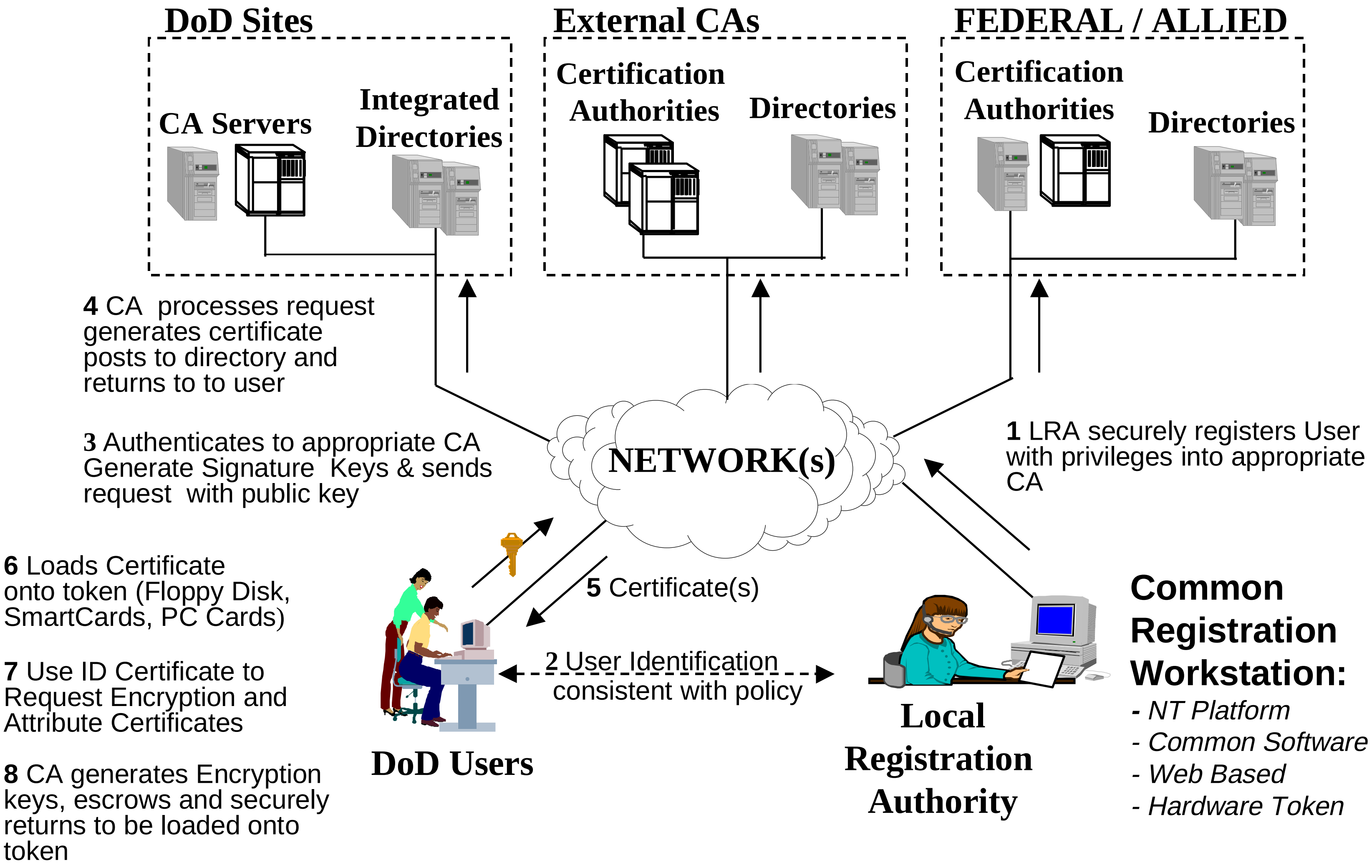
Target Goals & Objectives

- Appropriate security
  - Multiple Assurance Levels
- Make use of open standards based products and services
- Minimize Service resource impacts
  - common processes and components
  - minimum number of tokens
    - Today: Software & FORTEZZA
    - Future: SmartCards
- Ensure interoperability with external DOD partners
  - Federal / Allies / Commercial
- Long term goal of merging the DoD Key Management Systems (PKI, EKMS, others)

Target Architecture



Target User Registration



DoD Sites

CA Servers

Integrated Directories

External CAs

Certification Authorities

Directories

FEDERAL / ALLIED

Certification Authorities

Directories

NETWORK(s)

1 LRA securely registers User with privileges into appropriate CA

2 User Identification consistent with policy

3 Authenticates to appropriate CA Generate Signature Keys & sends request with public key

4 CA processes request generates certificate posts to directory and returns to to user

5 Certificate(s)

6 Loads Certificate onto token (Floppy Disk, SmartCards, PC Cards)

7 Use ID Certificate to Request Encryption and Attribute Certificates

8 CA generates Encryption keys, escrows and securely returns to be loaded onto token

DoD Users

Local Registration Authority

Common Registration Workstation:

- *NT Platform*
- *Common Software*
- *Web Based*
- *Hardware Token*

Technical Uncertainties
(Examples)

- Certificate Management Data Formats
  - Certificate & Certificate Revocation List (CRL) profiles
- Certificate policy processing / enforcement
- Access control
  - Discretionary with Identity Certificates
  - Mandatory with Attributes Certificates
- Interoperability
  - Cross certification
  - Multiple Roots
  - Subordinate CA
- Revocation
  - Online Certificate Status Protocol (OCSP)
  - Certificate Revocation List (CRL)
- Key Recovery Implementation
  - Application-based
  - Infrastructure-based
- Repository
  - Light-weight Directory Access Protocol (LDAP)
  - Directory Access Protocol (DAP)
  - Others

Strategy for establishing Target DOD PKI

- Define assurance levels and their usage (i.e. US DoD X.509 Certificate Policy)
- Develop the DoD PKI Strategy (I.e. Roadmap)
- Establish applications pilots using the current Medium Assurance PKI and External Certification Authorities (ECAs)
- Develop Information Assurance (IA) Framework Specifications for PKI components and applications
  - Functional and Security Testing
- Develop and Execute Acquisition Strategy
  - Based on analysis of pilot data and lessons learned

ASD(C3I) Policy Memorandum

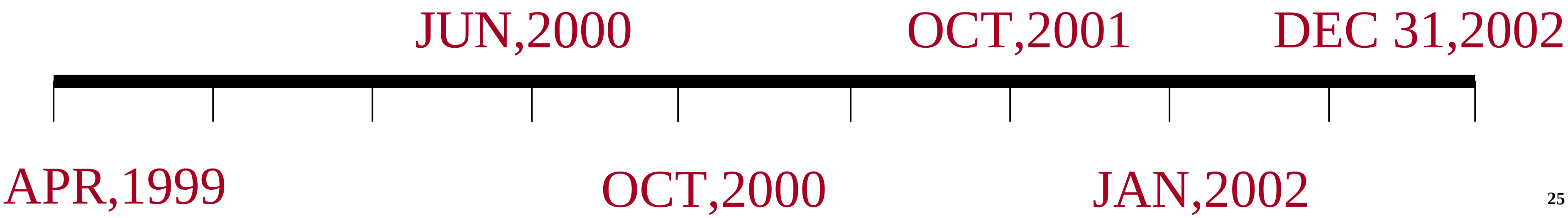
- DOD PKI Program Management Office (PMO) dated 9 April 99
  - Established a DOD PKI PMO
    - NSA named as the Program Manager
    - DISA named as the Deputy Program Manager
  - Requires a detailed implementation plan in 60 days

DOD PKI Policy Memorandum Timeline

APR,1999	START- Deploy Registration Capability Classes 3 & 4
JUN,2000	ALL Private WEB SERVERS shall have Class 3 or Class 4 certs
OCT,2000	FINISH- Deploy Reg. Cap. Class 3
OCT,2001	ALL DoD TO HAVE Class 3 certs, DoD WEB SERVERS Require Identification, All DoD E-mail to be signed
JAN,2002	START -Issuing Class 4 certs to Class 3 cert holders
DEC 31,2002	FINISH- All DoD to have Class 4 certs

LEGEND on TIMELINE

each mark is 5 Months



DoD PKI - Medium Assurance Website Information

- http://www.disa.mil/infosec/pki-int.html
  - DOD PKI Medium Assurance Interoperability
    - DOD PKI Medium Assurance X.509 v3 certificate standard profiles (formats and examples)
    - available to .mil; .gov; .edu; and .com
- http://iase.iiie.disa.mil
  - Information Assurance Support Environment
    - available to .mil; and .gov

Summary

- Target is an integrated DoD PKI with support for multiple assurance levels
- Increased integration between Assurance level components and services
- DoD programs requiring PKI support subscribe to DoD PKI rather than building stovepipes
- DoD to exercise technical & marketplace leadership
  - Develop PKI and related Information Assurance specifications and get out to industry ASAP
  - Specifications based on commercial standards to the greatest extent possible

Questions